NOTE ON THE CONGRUENCE $2^{4n} \equiv (-)^n (2n)!/(n!)^2$, WHERE $2n+1$ IS A PRIME.

By Prof. F. Morley, Haverford, Pa.

1. There are two ways of integrating $\cos^{2n+1} x dx$, one by a Fourier series, where we express $\cos^{2n+1} x$ in terms of cosines of multiples of x, the other by a "formula of reduction." Taking the integral from $x = 0$ to $x = \pi/2$, and equating the two forms of the integral, we have an algebraic identity, which will, on a suitable supposition as to the integer n, yield a theorem as to prime numbers, trivial or otherwise. Doing this, we have, first,

$$2^{2n} \cos^{2n+1} x = \cos (2n+1)x + (2n+1) \cos (2n-1) x$$

$$+ \frac{(2n+1).2n}{1.2} \cos (2n-3)x + \ldots + \frac{(2n+1)2n \ldots (n+2)}{n!} \cos x,$$

$$2^{2n} \int_0 \cos^{2n+1} x dx = \frac{\sin (2n+1)x}{2n+1} + \frac{2n+1}{2n-1} \sin (2n-1)x + \ldots,$$

$$2^{2n} \int_0^{\frac{1}{2}\pi} \cos^{2n+1} x dx = (-)^n \left\{ \frac{1}{2n+1} - \frac{2n+1}{2n-1} + \ldots \right\};$$

and second, from the formula of reduction,

$$\int_0^{\frac{1}{2}\pi} \cos^{2n+1} x dx = \frac{2n(2n-2)\ldots 2}{(2n+1)(2n-1)\ldots 3}; \tag{1}$$

so that the algebraic identity is

$$2^{2n} \frac{2n(2n-2)\ldots 2}{(2n+1)(2n-1)\ldots 3}$$

$$= (-)^n \left\{ \frac{1}{2n+1} - \frac{2n+1}{2n-1} + \frac{(2n+1)2n}{1.2(2n-3)} - \ldots + (-)^n \frac{(2n+1)2n\ldots(n+2)}{n!} \right\}.$$

Let $2n+1$ be a prime p. Let us use the notation $a/b \equiv 0$, mod c, where a/b is a *fraction*, to mean that when the fraction is in its lowest terms the numerator has the factor c. Then, from the above identity,

$$2^{2n} \frac{2n(2n-2)\ldots 2}{(2n+1)(2n-1)\ldots 3} - (-)^n \frac{1}{2n+1} \equiv 0, \text{ mod } p,$$

or

$$2^{2n} \frac{2n(2n-2)\ldots 2}{(2n-1)(2n-3)\ldots 1} - (-)^n \equiv 0, \text{ mod } p^2,$$

or

$$2^{4n}\frac{(n!)^2}{(2n)!} - (-)^n \equiv 0\,, \ \text{mod}\, p^2\,,$$

or

$$2^{4n} - (-)^n \frac{(2n)!}{(n!)^2} \equiv 0\,, \ \text{mod}\, p^2\,, \tag{2}$$

the left hand member being of course an integer.

This result is given in Mathews, Theory of Numbers, p. 318, Ex. 16.

When $n = 1, 2, 3$, the left hand member of (2) is respectively 18, 250, 4116, that is $2\,.\,3^2$, $2\,.\,5^3$, $2^2\,.\,3\,.\,7^3$. Thus, when $p = 5$ and 7, the left hand member $\equiv 0$, mod p^3, not merely mod p^2. I have to prove that this is so when p is a prime > 3.

2. It is convenient to prove, first, that when $p > 3$

$$\frac{1}{1^2} + \frac{1}{3^2} + \ldots + \frac{1}{(p-2)^2} \equiv 0\,, \ \text{mod}\, p\,. \tag{3}$$

Using the notation and results of Chrystal, Algebra, Vol. ii, p. 525, let

$$(x+1)(x+2)\ldots(x+p-1) = x^{p-1} + A_1 x^{p-2} + \ldots + A_{p-1}\,.$$

We have

$$[(p-1)!]^2 \left[\frac{1}{1^2} + \frac{1}{2^2} + \ldots + \frac{1}{(p-1)^2}\right] = A^2_{p-2} - 2A_{p-1}A_{p-3}\,;$$

or since $A_{p-2}, A_{p-3} \equiv 0$ mod p, if $p > 3$,

$$\frac{1}{1^2} + \frac{1}{2^2} + \ldots + \frac{1}{(p-1)^2} \equiv 0 \ \text{mod}\, p\,. \tag{4}$$

Now (writing always $2n + 1 = p$),

$$\frac{1}{1^2} - \frac{1}{(2n)^2} + \frac{1}{2^2} - \frac{1}{(2n-1)^2} + \ldots + \frac{1}{n^2} - \frac{1}{(n+1)^2}$$

$$= \frac{(2n)^2 - 1^2}{1^2(2n)^2} + \frac{(2n-1)^2 - 2^2}{2^2(2n-1)^2} + \ldots + \frac{(n+1)^2 - n^2}{n^2(n+1)^2} \equiv 0 \ \text{mod}\, p\,,$$

for each numerator has, and each denominator has not, the factor $2n + 1$.

Hence, both sum and difference of the expressions

$$\frac{1}{1^2} + \frac{1}{2^2} + \ldots + \frac{1}{n^2} \ \text{ and } \ \frac{1}{(n+1)^2} + \ldots + \frac{1}{(2n)^2}$$

$\equiv 0$, mod p; hence, also, each expression $\equiv 0$ mod p. Hence, again,

$$\frac{1}{2^2} + \frac{1}{4^2} + \ldots + \frac{1}{(2n)^2} \equiv 0\,, \ \text{mod}\, p\,.$$

Hence we can remove the even terms from the statement (4), and there remains (3).

3. Instead of expressing $\cos^p x$ as a sum of cosines, let us take the formula which expresses $\cos px$ as a power-series in $\cos x$. This is shown in treatises on trigonometry to be

$$(-)^n \cos px = p \cos x - \frac{p(p^2-1^2)}{3!} \cos^3 x + \frac{p(p^2-1^2)(p^2-3^2)}{5!} \cos^5 x - \dots$$
$$+ (-)^n 2^{p-1} \cos^p x .$$

Multiply by dx and integrate from 0 to $\frac{1}{2}\pi$; then, using (1),

$$\frac{1}{p} = p - \frac{p(p^2-1^2)}{3!} \frac{2}{3} + \frac{p(p^2-1^2)(p^2-3^2)}{5!} \frac{2 \cdot 4}{3 \cdot 5} + \dots$$
$$+ (-)^n 2^{p-1} \frac{2 \cdot 4 \dots (p-1)}{3 \cdot 5 \dots p} .$$

Therefore,

$$\frac{1}{p} - (-)^n 2^{p-1} \frac{2 \cdot 4 \dots (p-1)}{3 \cdot 5 \dots p} \equiv p \left\{ 1 + \frac{1}{3^2} + \frac{1}{5^2} + \dots + \frac{1}{(p-2^2)^2} \right\}, \bmod p^3$$

i. e. (Art. 2) $\equiv 0, \bmod p^2$.

Therefore

$$(-)^n 2^{p-1} \frac{2 \cdot 4 \dots (p-1)}{1 \cdot 3 \dots (p-2)} - 1 \equiv 0, \bmod p^3$$

whence, as in Art. 1,

$$2^{4n} - (-)^n \frac{(2n)!}{(n!)^2} \equiv 0, \bmod p^3,$$

where $2n+1$ is a prime p, greater than 3.

HAVERFORD COLLEGE, *Nov.* 5, 1895.